Update

on

1989 Guidelines

on

Facsimile Transmission Security

June 1990

TABLE OF CONTENTS

UPDATE ON 1989 FAX GUIDELINES

1. INTRODUCTION

1.1 Background

In June of 1989, the Office of the Information and Privacy Commissioner/Ontario (IPC) issued a set of guidelines for government institutions to consider when developing systems and procedures to maintain the confidentiality of information transmitted by facsimile (commonly referred to as "fax"). This document was entitled "Guidelines on Facsimile Transmission Security" (Guidelines). These Guidelines were issued to all institutions in Ontario that fell under the jurisdiction of the *Freedom of Information and Protection of Privacy Act, 1987*, as amended, (*Act*).

The response to the IPC Guidelines was extremely positive and hundreds of requests for the Guidelines were received from both Canadian and American organizations, in both the public and private sectors.

Effective January 1, 1991 all municipalities, agencies, local boards and commissions in Ontario will be required to comply with the *Municipal Freedom of Information and Protection of Privacy Act, 1989*. It is estimated that approximately, 3,000 institutions will be required to comply with this statute. Consequently, over 3,300 institutions in Ontario will be required to comply with provincial privacy regulations.

Primarily due to its great speed and convenience, the use of fax machines continues to proliferate. Based upon the results of a survey conducted by the IPC in March of 1990, we learned that 83 provincial government institutions made use of approximately 2,052 fax machines.

At the time of the its release, the IPC had decided to update the Guidelines in roughly one year. Taking these factors into consideration, the IPC chose to review its Guidelines in the spring of 1990.

1.2 Objectives of This Document

The purpose of this document is to review the Guidelines issued in 1989, to ensure that they are still appropriate in the context of generally available fax technology, and to provide an update of any new security-related developments.

1.3 Approach and Scope

A) The IPC decided to conduct a survey of the majority of provincial institutions that were issued the original Guidelines. The main objective of the survey was to obtain feedback from these institutions in order to assess how useful they found the Guidelines in their use of fax machines.

B) The Guidelines themselves were reviewed to ensure that they were still appropriate in the context of generally available fax technology. Any significantly new security features that are now generally available and that could assist in implementing the Guidelines, will be identified.

It is not the intention of this document to identify all the new fax-related products available. Nor do we intend to recommend or favour any particular product, brand name or vendor.

2. SURVEY OF INSTITUTIONS

2.1 Methodology

Most institutions under the jurisdiction of the *Act* were sent a fax survey questionnaire. Some institutions did not have their own fax machines, but used the services of an affiliated or related institution. In those instances, the office procedures of the affiliated or related institution were complied with.

The following is a summary of the survey responses:

	INSTITUTIONS	
	No.	%
Responded	83	33
Responded, but did not have own fax machine	32	13
No response	134	54
	249	100

Table 1 presents the distribution of fax machines among the institutions that responded to our survey questionnaire. Over half of these institutions had between one and four fax machines each. A quarter of the institutions fell into the category of having 20 or more fax machines.

2.2 Policies

Only 40% of the institutions that replied stated that they had a formal policy regarding the use of their fax machine (see Table 2). A number of these institutions replied that they had adopted the IPC guidelines. Some of the institutions which indicated they did not have a policy, stated that they were in the process of developing such a policy.

We considered institutions in the category of having 20 or more fax machines each, as a significant group. Among such institutions, 33% had a fax policy compared to the overall average of 40% for the entire group (Table 2). In light of the proliferation of fax machines, institutions should develop a policy on the use of fax machines in their organization (especially those with a significant number).

2.3 Office Procedures

Over half of the institutions replied that they had reviewed existing office procedures involving fax transmissions as a result of the IPC Guidelines (see Table 3). Others replied that they were in the process of doing so. Some institutions were unaware of the security implications of fax transmissions, while to others, the IPC Guidelines reinforced their concerns over the security of such transmissions. Eighty-four percent of the institutions that responded stated that the Guidelines were useful as a reference document for designing new procedures (see Table 4). Thirty-eight percent of the larger institutions (with 20 or more fax machines) indicated that the Guidelines had triggered them to review their security in other areas as well, such as local area networks of computers (see Table 5). Reviewing overall security in a number of areas appears to be an ongoing process.

2.4 Security Features

Over one-third of the institutions responded that the Guidelines had caused them to review existing features on their fax machines (see Table 6). Some of the institutions indicated that they had not done so because they were already aware of the security problems associated with fax transmissions. It is encouraging to note that over half of the institutions with 20 or more fax machines had done so. Some institutions indicated that such a review was scheduled to be conducted in the near future. Forty-one percent of all institutions found the IPC Guidelines to be a useful reference for specifying features when ordering new fax machines or upgrading their existing ones (see Table 7). The most common security features used by institutions were confidential mailboxes and the placement of fax machines in secure locations.

2.5 Third Party Communication

Thirty percent of the institutions that replied estimated that over half of their fax activity was with third parties (see Table 8). Some were unable to make this estimate in time for our survey. We defined third parties as those organizations that are not required to comply with Ontario's access and privacy legislation. Institutions with the major portion of their fax activity transmitted to third parties have an additional responsibility to ensure that personal information is faxed securely. Once transmitted outside of the *Act*'s jurisdiction, such information can no longer be protected by the *Act*.

3. REVIEW OF 1989 FAX GUIDELINES

3.1 Technology

It is our opinion that encrypting or encoding information is the most effective means of protecting it from being intercepted and read by unauthorized persons, during electronic transmissions.

The practical problems that existed with encryption in the past, still remain. Fax machines that have internal encryption devices may only transmit encrypted information to identical fax machines in the user group. External encryption devices are now available which can be attached to a fax machine. However, this solution still requires that the identical encryption device be available on all fax machines in the user group.

An additional problem with encryption is the need for a special code or encryption key which must be generated and distributed to all fax encryptors in the user group. The encryption key must be distributed by a secure method such as by courier. This procedure must be followed each time that the key is changed. This practical problem of encryption key management has now been resolved through the availability of encryption devices which use automatic encryption and key management techniques.

The Guidelines recognized that encrypted information could also be transmitted between computers and then decrypted or decoded at the receiving computer. The practical problem identified in using this procedure, namely that all the information required to be faxed may not be stored on the computer, still remains. For example, records such as the minutes of meetings, correspondence, or handwritten notes, may not be stored on the sender's computer.

Thus, under existing commercially available fax technology, encryption still does not appear to be a satisfactory solution for most "normal" situations. Where practical, however, we encourage consideration of its use when faxing very sensitive personal information, since it remains the most secure method of transmission.

In February of 1990, Ontario's Management Board of Cabinet issued, "A Directive For The Management Of Information Technology Security". One of its purposes was to ensure that ministries safeguarded the confidentiality, integrity and availability of their data while it was created, stored, processed or communicated through information technology, including fax machines. One of the principles specified in this document was that: "Information technology security is to be consistent with the privacy and confidentiality requirements of the *Freedom of Information and Protection of Privacy Act*." This indicates that privacy principles will form a key component on information technology security developments in the public sector, and is consistent with the Guidelines established by the IPC for the use of fax technology.

3.2 Capabilities of Fax Machines

Our Guidelines identified three existing features on fax machines that would provide certain levels of control over fax transmission security:

- Keylocks;
- Confidential Mailboxes; and
- Activity Confirmation Reports.

Existing capabilities of fax machines have not fundamentally changed in the area of transmission security. Therefore, the features identified above still remain. We refer readers to the 1989 Guidelines for a detailed description of the above controls.

3.3 User Procedures

Like telephone conversations, fax transmissions may be "tapped" or intercepted. Practically, however, the major security risk is that the sender will dial an incorrect fax number or that the faxed message will not be delivered to the intended recipient. In order to control for this risk (absent the security measures associated with fax machines discussed earlier), secure fax transmissions are largely dependant on having adequate policies and user procedures, while utilizing the existing features on the machine to their utmost. Adequate user procedures formed the fundamental premise underlying our original Guidelines, and continue to do so at present.

In the following section, we wish to apprise readers of possible practices used by other institutions and organizations to enhance their fax transmission security.

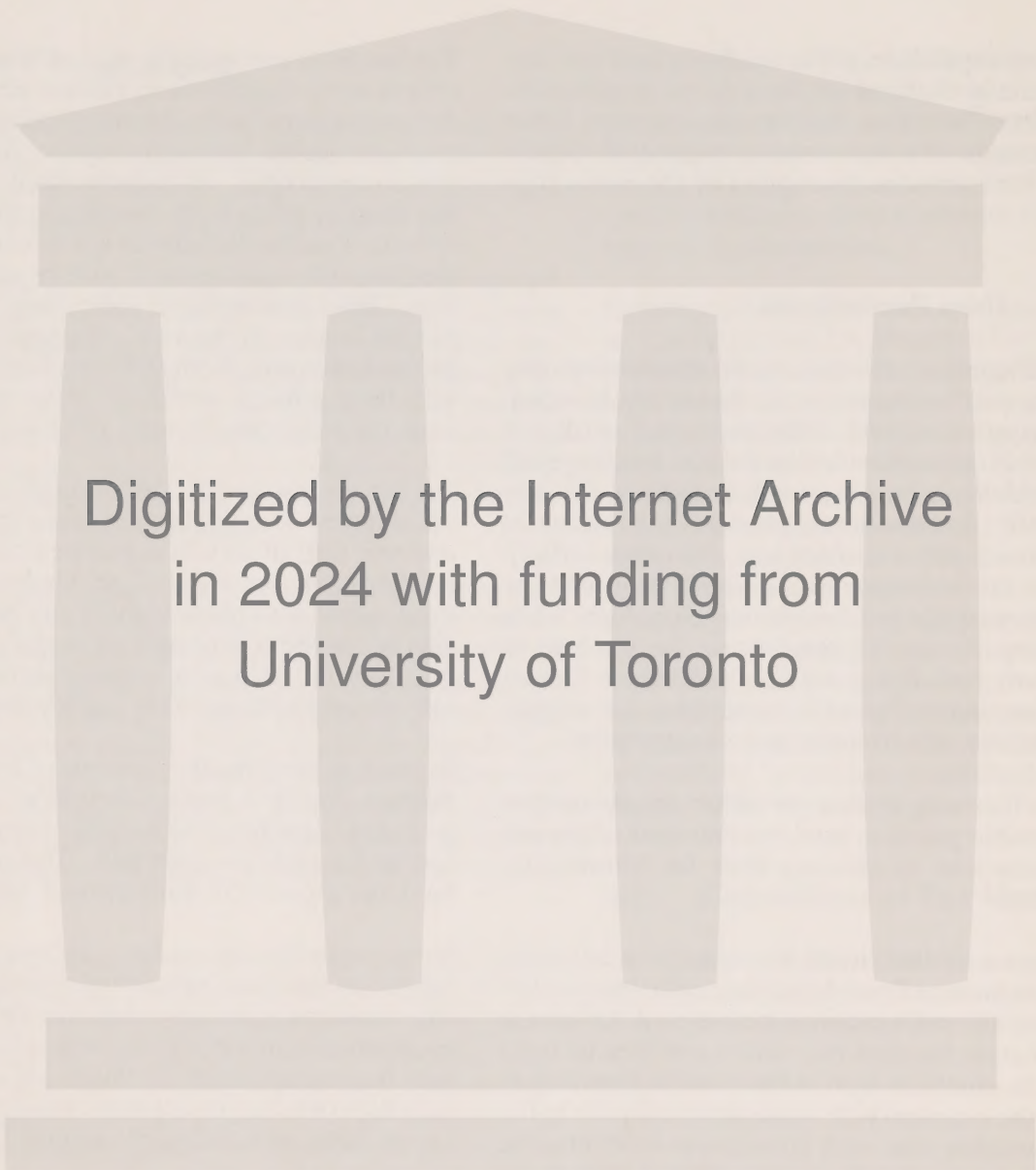
There are certain situations where personal information must be faxed by an institution because the personal identifiers cannot be removed. Often, the destination fax does not have a confidential mailbox. In situations such as these, institutions should alert the recipient with a telephone call prior to the transmission, that such information is about to be faxed and to await its receipt. Once received, the recipient should confirm receipt by telephone.

Fax machines use specially treated thermographic or heat-printed paper to record incoming messages. After a number of years, thermographic paper tends to be unreadable, leading to the loss of the information recorded on it. Institutions should photocopy information printed on thermographic paper in order to preserve the information contained therein long enough to correspond with its retention period. The thermographic paper may then be destroyed in a secure manner. Messages printed on fax machines using thermal ink transfer or equipped with laser printers would not have this problem since thermographic paper is not used.

Institutions may receive fax messages after normal office hours. During this time, security may be lax and only staff of certain departments such as data processing may be in the office. Under such conditions, some institutions identify and isolate a specific fax machine to receive messages after normal office hours. Such a fax machine should be physically secured from access by unauthorized persons.

In order to preserve the contents of a confidential mailbox during a power disruption, some users provide fax machines with a more permanent storage device such as a hard disk. The contents of a hard disk are not lost during power failures.

Some organizations conduct a risk analysis on the type of information transmitted or received by fax. The entire organization or a particular branch that faxes sensitive or confidential personal information may become classified as "high risk". Entities in such high risk categories will then be provided with fax machines with additional security features.



APPENDIX:

TABLES

TABLE 1

DISTRIBUTION OF FAX MACHINES

MACHINES	INSTITUTIONS No.	%
1	34	41
2-4	15	18
5-9	6	7
10-19	7	9
20-39	2	2
40-59	6	7
60-79	4	5
80-99	2	2
100 & Over	7	9
TOTAL	83	100

TABLE 2

INSTITUTIONS WITH A FAX POLICY

MACHINES	INSTITUTIONS	HAD POLICY No.	HAD POLICY %
1	34	13	38
2-4	15	7	47
5-9	6	3	50
10-19	7	3	43
20-39	2	1	50
40-59	6	2	33
60-79	4	1	25
80-99	2	1	50
100 & Over	7	2	29
TOTAL	83	33	40

TABLE 3

REVIEWED EXISTING PROCEDURES

MACHINES	INSTITUTIONS	PROCEDURES	
		No.	%
1	34	17	50
2-4	15	9	60
5-9	6	3	50
10-19	7	4	57
20-39	2	1	50
40-59	6	3	50
60-79	4	1	25
80-99	2	2	100
100 & Over	7	3	43
TOTAL	83	43	52

TABLE 4

USEFUL WHEN DESIGNING NEW PROCEDURES

MACHINES	INSTITUTIONS	USEFUL		NOT USEFUL	
		No.	%	No.	%
1	21	15	71	6	29
2-4	10	8	80	2	20
5-9	3	3	100	0	0
10-19	7	6	86	1	14
20-39	2	2	100	0	0
40-59	4	4	100	0	0
60-79	2	2	100	0	0
80-99	2	2	100	0	0
100 & Over	5	5	100	0	0
TOTAL	56	47	84	9	16

TABLE 5

INSTITUTIONS THAT REVIEWED OTHER AREAS

MACHINES	INSTITUTIONS	REVIEWED OTHER AREAS	
		No.	%
1	34	2	6
2-4	15	2	13
5-9	6	0	0
10-19	7	2	29
20-39	2	1	50
40-59	6	2	33
60-79	4	2	50
80-99	2	1	50
100 & Over	7	2	29
TOTAL	83	14	17

TABLE 6

INSTITUTIONS THAT REVIEWED EXISTING FEATURES

MACHINES	INSTITUTIONS	REVIEWED	
		No.	%
1	34	10	29
2-4	15	8	53
5-9	6	0	0
10-19	7	1	14
20-39	2	1	50
40-59	6	4	67
60-79	4	2	50
80-99	2	1	50
100 & Over	7	5	71
TOTAL	83	32	39

TABLE 7

USEFUL IN PURCHASING NEW MACHINES

MACHINES	INSTITUTIONS	USEFUL	
		No.	%
1	34	11	32
2-4	15	8	53
5-9	6	1	17
10-19	7	1	14
20-39	2	1	50
40-59	6	4	67
60-79	4	3	75
80-99	2	0	0
100 & Over	7	5	71
TOTAL	83	34	41

TABLE 8

OVER 50% OF FAX ACTIVITY WITH THIRD PARTIES

MACHINES	INSTITUTIONS	OVER 50%	
		No.	%
1	34	10	29
2-4	15	9	60
5-9	6	0	0
10-19	7	1	14
20-39	2	1	50
40-59	6	3	50
60-79	4	0	0
80-99	2	0	0
100 & Over	7	1	14
TOTAL	83	25	30

TABLEAU 8

Plus de 50 % des transmissions par télécopieur effectuées avec des tiers

TÉLÉCOPIEURS	INSTITUTIONS	PLUS DE 50%	
		Nombre	%
1	34	10	29
2-4	15	9	60
5-9	6	0	0
10-19	7	1	14
20-39	2	1	50
40-59	6	3	50
60-79	4	0	0
80-99	2	0	0
100 et plus	7	1	14
TOTAL	83	25	30

TABLEAU 7

Utilité des directives à l'achat de machines neuves

TÉLÉCOPIEURS	INSTITUTIONS	UTILES	
		Nombre	%
1	34	11	32
2-4	15	8	53
5-9	6	1	17
10-19	7	1	14
20-39	2	1	50
40-59	6	4	67
60-79	4	3	75
80-99	2	0	0
100 et plus	7	5	71
TOTAL	83	34	41

TABLEAU 6

Institutions ayant étudie les dispositifs existants

TÉLÉCOPIEURS	INSTITUTIONS	ÉTUDIÉS	
		Nombre	%
1	34	10	29
2-4	15	8	53
5-9	6	0	0
10-19	7	1	14
20-39	2	1	50
40-59	6	4	67
60-79	4	2	50
80-99	2	1	50
100 et plus	7	5	71
TOTAL	83	32	39

TABLEAU 5

Institutions ayant révisé d'autres domaines

TÉLÉCOPIEURS	INSTITUTIONS	RÉVISÉ D'AUTRES DOMAINES	
		Nombre	%
1	34	2	6
2-4	15	2	13
5-9	6	0	0
10-19	7	2	29
20-39	2	1	50
40-59	6	2	33
60-79	4	2	50
80-99	2	1	50
100 et plus	7	2	29
TOTAL	83	14	17

TABLEAU 4

Directives utiles à l'élaboration de nouvelles méthodes

TÉLÉCOPIEURS	INSTITUTIONS	UTILES		INUTILES	
		Nombre	%	Nombre	%
1	21	15	71	6	29
2-4	10	8	80	2	20
5-9	3	3	100	0	0
10-19	7	6	86	1	14
20-39	2	2	100	0	0
40-59	4	4	100	0	0
60-79	2	2	100	0	0
80-99	2	2	100	0	0
100 et plus	5	5	100	0	0
TOTAL	56	47	84	9	16

TABLEAU 3

Institutions ayant leurs méthodes existantes

TÉLÉCOPIEURS	INSTITUTIONS	MÉTHODES	
		Nombre	%
1	34	17	50
2-4	15	9	60
5-9	6	3	50
10-19	7	4	57
20-39	2	1	50
40-59	6	3	50
60-79	4	1	25
80-99	2	2	100
100 et plus	7	3	43
TOTAL	83	43	52

TABLEAU 2

Institutions dotées de règles relatives à la transmission par télécopieur.

TÉLÉCOPIEURS	INSTITUTIONS	DISPOSENT DE REGLES	
		Nombre	%
1	34	13	38
2-4	15	7	47
5-9	6	3	50
10-19	7	3	43
20-39	2	1	50
40-59	6	2	33
60-79	4	1	25
80-99	2	1	50
100 et plus	7	2	29
TOTAL	83	33	40

TABLEAU 1

RÉPARTITION DES TÉLÉCOPIEURS

TÉLÉCOPIEURS	INSTITUTIONS	
	Nombre	%
1	34	41
2-4	15	18
5-9	6	7
10-19	7	9
20-39	2	2
40-59	6	7
60-79	4	5
80-99	2	2
100 et plus	7	9
TOTAL	83	100

ANNEXE:

TABLEAUX

3.3 Méthodes d'utilisation

Tout comme pour une conversation téléphonique, une transmission par télécopieur peut être captée et interceptée. En pratique, le plus gros risque est cependant que l'expéditeur compose le mauvais numéro de télécopieur ou qu'un message télécopié n'atteigne pas le destinataire voulu. Pour éviter ce risque (en l'absence des mesures de sécurité dont nous avons parlé plus haut), la transmission sécuritaire par télécopieur dépend largement de règles et de méthodes d'utilisation adéquates, en plus de l'utilisation au maximum des dispositifs dont sont dotés les télécopieurs. Le recours à des méthodes d'utilisation adéquates était le message central de nos directives originales, et continue de l'être.

Dans la section suivante, nous porterons à la connaissance de nos lecteurs des méthodes intéressantes employées par d'autres institutions et organismes pour rehausser la sécurité de leurs transmissions par télécopieur.

Dans certains cas, une institution doit transmettre par télécopieur des renseignements personnels dont elle ne peut extraire les indices permettant d'identifier les personnes en cause. Il arrive souvent que le télécopieur récepteur n'ait pas de boîtes à lettres confidentielle. Dans ces cas-là, les institutions se doivent d'avertir le destinataire par téléphone avant la transmission qu'elles sont sur le point de lui transmettre de tels renseignements par télécopieur, et qu'il doit en attendre la réception. Par la suite, le destinataire doit leur confirmer la réception par téléphone.

Les télécopieurs enregistrent les messages qu'ils reçoivent sur du papier thermographique spécialement traité. Après un certain nombre d'années, le papier thermographique tend à devenir illisible, ce qui entraîne la perte des renseignements qu'il comporte. Les institutions feraient bien de photocopier les renseignements imprimés sur papier thermographique pour pouvoir les préserver durant toute la période prescrite de leur conservation. Le papier thermographique peut alors être détruit d'une manière sécuritaire. Les messages imprimés sur télécopieurs ayant recours au transfert d'encre thermal ou connectés à une imprimante au laser ne présenteraient pas ce problème puisqu'ils ne sont pas imprimés sur du papier thermographique.

Les institutions peuvent recevoir des messages par télécopieur lorsque leurs bureaux sont fermés. ¨ ce moment-là, la sécurité peut être relâchée et seul le personnel de certains services, comme ceux du traitement des données, peut être encore au travail. Dans ces cas, certaines institutions désignent et isolent un télécopieur destiné à recevoir les messages en dehors de leurs heures d'ouverture. Un tel télécopieur doit être inaccessible aux personnes non autorisées.

Pour préserver le contenu d'une boîte à lettres confidentielle en cas de panne d'électricité, certains utilisateurs dotent leur télécopieur d'un dispositif de stockage plus permanent, comme un disque dur. Le contenu d'un disque dur ne se perd pas durant une panne d'électricité.

Certains organismes soumettent le genre de renseignements transmis ou reçus par télécopieur à une analyse de risques. L'ensemble de l'organisme ou un service particulier qui transmet des renseignements personnels de nature délicate ou confidentielle par télécopieur pourrait être classé comme «risque élevé». On pourrait alors doter cette catégorie de télécopieurs munis de dispositifs de sécurité supplémentaires.

3. RÉVISION DES DIRECTIVES

3.1 Technologie

À notre avis, le chiffrement ou le codage des renseignements constitue le moyen le plus efficace d'empêcher leur interception et leur lecture par des personnes non autorisées au cours de la transmission électronique.

Les problèmes d'ordre pratique concernant le chiffrement sont toujours présents. Les télécopieurs équipés d'un dispositif interne de chiffrement ne peuvent transmettre des renseignements chiffrés qu'à des télécopieurs identiques du groupe utilisateur. Il existe maintenant des dispositifs externes que l'on peut adapter aux télécopieurs. Mais cette solution exige toujours que l'on dote du même dispositif de chiffrement tous les télécopieurs du groupe utilisateur.

Le chiffrement pose un autre problème : il faut produire une clé de chiffrement ou de codage spéciale et la distribuer à toutes les unités de chiffrement du groupe utilisateur d'une manière sécuritaire, par messager par exemple. On doit procéder ainsi chaque fois que l'on change la clé de chiffrement. Ce problème pratique de la gestion des clés de chiffrement est maintenant résolu grâce à des dispositifs de chiffrage qui font appel à des techniques automatisées de gestion du chiffrement et des clés y afférentes.

Les directives mentionnent que l'on peut également transmettre des renseignements chiffrés d'un ordinateur à l'autre, à déchiffrer et à décoder par l'ordinateur récepteur. Ce procédé présente cependant un problème en ce sens que tous les renseignements à télécopier peuvent ne pas être gardés sur ordinateur. Par exemple, des textes comme des procès-verbaux de réunions et autres documents manuscrits ne peuvent être conservés dans l'ordinateur de l'expéditeur.

Compte tenu de la technologie actuelle de transmission par télécopieur, le chiffrement ne semble donc pas convenir dans la plupart des cas courants. Nous encourageons cependant ceux qui le peuvent à l'utiliser pour transmettre des renseignements de nature très délicate, puisque ce moyen reste la méthode de transmission la plus sûre.

En février 1990, le Conseil de gestion du gouvernement de l'Ontario publiait un document intitulé «A Directive For The Management Of Information Technology Security». L'un des objectifs du document était de s'assurer que les ministères protègent l'intégrité, la disponibilité et le caractère confidentiel de leurs données au cours de leur création, de leur stockage, de leur traitement ou de leur communication au moyen de la technologie informatisée, y compris les télécopieurs. Un des principes précisé dans ce document était que «la sécurité de la technologie de l'information doit être conforme aux exigences de la *Loi sur l'accès à l'information et la protection de la vie privée* sur le plan de la confidentialité et de la protection de la vie privée». Cela explique pourquoi les principes relatifs à la protection de la vie privée formeront un élément clé de l'évolution de la sécurité des techniques de l'information dans le secteur public, conformément aux directives établies par le Bureau pour l'utilisation de la technologie de la transmission par télécopieur.

3.2 Capacité des télécopieurs

Nos directives mentionnent trois dispositifs courants des télécopieurs, qui offrent un certain degré d'assurance quant à la sécurité de la transmission des documents. Ce sont :

- les verrous de sécurité;
- les boîtes à lettres confidentielles; et
- les rapports de confirmation des mouvements du télécopieur.

La capacité actuelle des télécopieurs n'a pas beaucoup changé sur le plan de la sécurité de la transmission. Par conséquent, les dispositifs susmentionnés restent les mêmes. Nous renvoyons nos lecteurs aux directives de 1989 pour une description détaillée des dispositifs en question.

sécurité, alors que, pour d'autres, les directives du Bureau ont renforcé leur souci d'assurer la sécurité de telles transmissions. Selon 84 pour 100 des institutions qui ont répondu au questionnaire, les directives sont un document utile dans l'élaboration de leurs propres méthodes (voir tableau 4). Trente-huit pour cent des institutions plus importantes, dotées de 20 télécopieurs ou plus, ont indiqué que les directives les avaient incitées à examiner la question de sécurité dans d'autres domaines, tels que les réseaux locaux d'ordinateurs (voir tableau 5). L'examen de la sécurité d'ensemble dans un certain nombre de domaines semble être un processus continu.

2.4 Dispositifs de sécurité

Plus d'un tiers des institutions interrogées ont répondu que les directives les avaient incitées à examiner les dispositifs existants de leurs télécopieurs (voir tableau 6). D'autres institutions ont indiqué qu'elles ne l'avaient pas fait parce qu'elles étaient déjà conscientes des problèmes de sécurité associés aux transmissions par télécopieur. Il est encourageant de constater que plus de la moitié des institutions dotées de 20 télécopieurs ou plus l'ont fait. Quelques institutions ont indiqué qu'elles prévoyaient procéder à un tel examen dans un avenir prochain. Pour 41 pour 100 des institutions, les directives du Bureau sont un guide qui leur sera utile au moment de commander des télécopieurs neufs ou de moderniser les machines existantes (voir tableau 7). Les dispositifs de sécurité les plus couramment utilisés par les institutions sont les boîtes à lettres confidentielles et l'installation des télécopieurs dans un endroit protégé.

2.5 Communication avec des tiers

Trente pour cent des institutions qui ont répondu au questionnaire ont estimé que plus de la moitié de leurs communications par télécopieur concernaient des tiers (voir tableau 8). Certaines n'ont pas pu nous donner une estimation à temps pour notre enquête. Nous avons défini les tiers comme étant les organismes qui ne sont pas obligés d'obéir à la *Loi sur l'accès à l'information et la protection de la vie privée*. Les institutions qui transmettent la majeure partie de leurs documents à des tiers doivent prendre des précautions supplémentaires pour s'assurer de la transmission sécuritaire des renseignements personnels. En effet, la *loi* ne peut protéger les renseignements qui sortent de son champ d'application.

2. ENQUÊTE AUPRÈS DES INSTITUTIONS

2.1 Méthodologie

La plupart des institutions visées par la *loi* ont reçu un questionnaire relatif à la transmission par télécopieur. Certaines institutions qui n'ont pas leur propre télécopieur utilisent les services d'une institution affiliée ou connexe. Dans ces cas, ce sont les méthodes de travail de l'institution affiliée ou connexe que visait le questionnaire.

Voici un sommaire des réponses au questionnaire :

INSTITUTIONS

	Nombre	%
Ont répondu	83	33
Ont répondu, mais n'avaient pas leur propre télécopieur	32	13
N'ont pas répondu	134	54
	249	100

Le tableau 1 indique la répartition de télécopieurs parmi les institutions qui ont répondu à notre questionnaire. Plus de la moitié de ces institutions ont entre un et quatre télécopieurs chacune. Un quart des institutions entrent dans la catégorie de celles qui ont 20 télécopieurs ou plus.

2.2 Règles

Quarante pour cent seulement des institutions qui ont répondu au questionnaire déclarent qu'elles disposent de règles officielles concernant l'utilisation de leur télécopieur (voir tableau 2). Un certain nombre d'entre elles précisent avoir adopté les directives du Bureau. Plusieurs des institutions qui ont indiqué ne pas avoir de règles précises en la matière ont déclaré qu'elles étaient en train de les élaborer.

Les institutions de 20 télécopieurs ou plus nous semblent un groupe important; 33 pour 100 d'entre elles ont une règle sur l'utilisation des télécopieurs alors que la moyenne totale est de 40 pour 100 pour l'ensemble du groupe (tableau 2). Étant donné la prolifération des télécopieurs, les institutions doivent se doter de règles sur l'utilisation des télécopieurs dans leur organisation respective, surtout celles qui en possèdent un grand nombre.

2.3 Méthodes de travail

Plus de la moitié des institutions ont répondu qu'elles avaient révisé leurs méthodes de travail existantes en matière de transmission par télécopieur à la suite des directives du Bureau (voir tableau 3). D'autres ont répondu qu'elles étaient en train de le faire. Quelques-unes ignoraient les répercussions de la transmission par télécopieur en matière de

Mise à jour des directives de télécopieur de 1989

1. INTRODUCTION

1.1 Rappel des faits

En juin 1989, le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario publiait un document ayant pour objet de proposer aux institutions gouvernementales des directives aptes à les guider dans l'élaboration de systèmes et de méthodes visant à maintenir le caractère confidentiel des documents transmis par télécopieur. Il s'agit des «Directives concernant la sécurité de la transmission par télécopieur». Ces directives ont été envoyées à toutes les institutions de l'Ontario entrant dans le champ d'application de la *Loi de 1987 sur l'accès à l'information et la protection de la vie privée*, dans sa version modifiée.

Les directives ont reçu un accueil très favorable : des centaines d'organismes canadiens et américains, du secteur public comme du secteur privé, nous en ont demandé un exemplaire.

À compter du 1er janvier 1991, toutes les municipalités, organismes, commissions et conseils locaux de l'Ontario seront tenus d'observer la *Loi de 1989 sur l'accès à l'information municipale et la protection de la vie privée*. On estime à 3 000 environ le nombre des institutions qui seront tenues de s'y conformer. Plus de 3 300 institutions en Ontario devront donc observer les règlements provinciaux concernant la protection de la vie privée.

Étant donné la grande rapidité et la commodité de ces machines, l'utilisation des télécopieurs se répand de plus en plus. D'après les résultats d'un sondage mené par le Bureau du commissaire à l'information et à la protection de la vie privée en mars 1990, nous avons appris que 83 institutions du gouvernement provincial utilisaient quelque 2 052 télécopieurs.

Lors de la publication des directives, le Bureau du commissaire à l'information et à la protection de la vie privée avait annoncé sa décision de procéder à une mise à jour du document dans l'année qui suivait. En considération de quoi, le Bureau a révisé ses directives au printemps de 1990.

1.2 Objet du présent document

Le présent document a pour objet d'examiner les directives publiées en 1989 pour voir si elles tiennent compte des derniers progrès de la technologie de la transmission par télécopieur, et pour offrir une mise au point des derniers rebondissements en matière de sécurité.

1.3 Méthodes et portée de l'enquête

A) Le Bureau a décidé de mener une enquête auprès de la majorité des institutions provinciales qui ont reçu la première version des directives. L'enquête avait principalement pour objet d'obtenir des observations de ces institutions pour évaluer l'utilité des directives dans leur emploi des télécopieurs.

B) Le Bureau a étudié les directives pour s'assurer qu'elles tiennent compte des derniers progrès de la technologie de la transmission par télécopieur. Nous signalerons tout nouveau dispositif de sécurité important, offert sur le marché, qui pourrait faciliter la mise en application des directives.

Le présent document n'a pas pour objet d'identifier tous les nouveaux produits existant sur le marché de la transmission par télécopieur, pas plus qu'il ne vise à recommander ou favoriser un produit, une marque ou un vendeur quelconque.

TABLE DES MATIÈRES

Mise à jour

des

directives de 1989

concernant

la sécurité de la transmission

par télécopieur

Juin 1990